Purpose

The purpose of this guideline is to protect Ecology's existing IT infrastructure, applications, and staff resources from unintended consequences caused by the development, modification and/or installation of software on the Agency's IT architecture.

Background

The mission of the Department of Ecology is to protect, preserve and enhance Washington's environment, and promote the wise management of our air, land and water. In support of this mission the collection and use of data in automated systems has become routine. It has become critical to Ecology's business processes that the Agency's IT infrastructure and applications are functional and accessible during normal business hours.

Over time the Ecology's IT infrastructure and applications have grown increasingly complex. This is due in part to the growth in the number of servers and applications but current trends in application design (OO, SOA, etc.) are also major contributors. Unintended consequences to existing applications have occurred when new applications have been implemented or existing applications modified. Although Ecology staff has also caused problems, contracted IT consultants are more likely to introduce these issues. This wastes expensive contractor and Ecology IT resources and has caused deployment delays.

Audience

These guidelines apply to all IT consultants that are, or may be, developing and/or implementing software applications where any component of the application is targeted to reside on, or utilize, any server or service that is owned or administered by the Applications and Data Services Section (ADS). This includes but is not limited to, all ADS owned or administered application, web, database, or GIS servers regardless of where they are physically located or to which domain they belong. The Agency's data administration standards continue to be in effect for all database related activities.

Goals

The primary goals of these guidelines are to:

- Increase contractor understanding of Ecology's IT goals, organization and Infrastructure.

- Stimulate early and frequent communication between contracted IT consultants and Ecology staff responsible for Ecology's IT infrastructure and existing applications.

Guidelines

The IT industry continues to evolve at a very rapid pace. As with many organizations Ecology struggles to keep pace with the continuous changes. As a result these guidelines should not be taken as comprehensive or complete. They are meant to provide a starting point to stimulate communication prior to the design and development of applications.

General
- Open the lines of communication as soon as possible.
  - ADS Manager – Debbie Stewart
    - Phone - (360) 407-4078
    - E-mail – dste461@ecy.wa.gov
  - Database & Data Administration
    - E-mail – DBADMINS@ecy.wa.gov
  - Application & Server Administration
    - E-mail - ECYDLADSWBADMINS@ecy.wa.gov
- Any standard or guideline referenced or included in these guidelines may be out of date and should be verified before beginning work.

Infrastructure
- See the **Overview of Infrastructure** section of the Agency's It portfolio. (**http://www.ecy.wa.gov/services/as/it_portfolio/1_overview.htm#C**)

Development

- Use of Beta software for development is prohibited however exceptions may be made to meet critical business requirements.
- Installation of new or upgrades to existing software required by an application should not be taken for granted and must be approved.
- Configuration changes to Ecology servers and software should also not be taken for granted and must be approved.
- Applications should not be written in a manner to require Administrator privileges on the server.
- Use of Stored Procedures is required.
- Avoid the following bad practices:
  - Use of Embedded SQL
  - ODBC/DSN type of connections
  - Hard coded of folder paths

Deployment

- All applications must be deployed to the Agency's Dev/Test platform prior to being deployed to the Production platform.
- A WEB Application Installation/Deployment Form must be completed for all new applications and must be updated as needed for existing applications. This form can be found on the Agency's intranet or will be supplied upon request.

Security:

- Intranet based applications that modify databases or restrict access to existing data are required to utilize the Agency's in-house developed security application.
- The use of embedded logins or passwords is prohibited.
- Applications must be designed in a manner to prevent unauthorized alteration of code or content.
- The in-house use of contractor supplied equipment must be approved prior to connection to the Agency's network.